

AO 106 (Rev. 04/010) Application for Search Warrant

AUTHORIZED AND APPROVED/DATE: CB 12/14/2023

## UNITED STATES DISTRICT COURT

AMG  
12/14/23

WESTERN

for the  
DISTRICT OF

OKLAHOMA

In the Matter of the Search of )  
 )  
 green iPhone 13 Pro Max, sn # D479F6MK4C )  
 EMEI # 350776591837361; )  
 A brown Delsey Paris Backpack; )  
 A black and brown Samsonite rolling hardside )  
 luggage bag; )  
 A blue Samsonite soft luggage bag )

Case No: M-23-1018-AMG

## APPLICATION FOR SEARCH WARRANT

I, Wes Gillespie, a federal law enforcement officer or attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following property (*identify the person or describe property to be searched and give its location*):

See Attachment A

Located in the Western District of Oklahoma, there is now concealed (*identify the person or describe the property to be seized*):

See Attachment B

The basis for the search under Fed. R. Crim.P.41(c) is(*check one or more*):

- ☒ evidence of the crime;  
☒ contraband, fruits of crime, or other items illegally possessed;  
☒ property designed for use, intended for use, or used in committing a crime;  
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

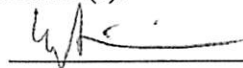
Code Section  
 18 U.S.C. § 371  
 18 U.S.C. § 2113(b)

Offense Description  
 Conspiracy  
 Bank Theft

The application is based on these facts:

See attached Affidavit of Special Agent Wesley Gillespie, United States Secret Service, which is incorporated by reference herein.

- ☒ Continued on the attached sheet(s).  
☐ Delayed notice of [No. of Days] days (*give exact ending date if more than 30 days*) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet(s).



Applicant's signature

Wesley Gillespie  
 SA  
 USSS

Sworn to before me and signed in my presence.

Date: 12/14/23

City and State: Oklahoma City, Oklahoma

  
*Judge's signature*

AMANDA MAXFIELD GREEN, U.S. Magistrate Judge  
*Printed name and title*

## **AFFIDAVIT IN SUPPORT OF SEARCH WARRANT**

I, Wesley Gillespie, a Special Agent with the United States Secret Service, being duly sworn, hereby depose and state as follows:

### **Introduction**

1. I have been a Special Agent with the United States Secret Service since March 2003. I am currently the Team Leader for the Cyber Crimes Task Force (the “task force”). I specialize in investigating financial crimes, including wire fraud, bank fraud, identity theft, cyber fraud, payment terminal attacks, and ATM jackpotting. I have conducted investigations involving criminal violations of Title 18 of the United States Code, including bank fraud, bank theft, wire fraud, and computer crimes.

2. I am experienced in executing search and arrest warrants as well as debriefing defendants, witnesses, informants, and other persons who have knowledge of specific crimes in violation of Title 18 of the United States Code.

3. I present this affidavit in support of an application for a warrant to search a green iPhone 13 Pro Max bearing serial # D479F6MK4C and EMEI # 350776591837361 (“the subject device”), a brown Delsey Paris backpack, a black and brown Samsonite rolling hardside luggage bag, and a blue Samsonite soft luggage bag (“the subject bags”), located at the United States Secret Service Oklahoma City Field Office at 210 Park Ave, Suite 1100, Oklahoma City, Oklahoma. This affidavit sets forth facts to establish probable cause to believe that evidence, fruits, and instrumentalities of illegal activity in violation of, among other statutes, 18 U.S.C. § 371 (conspiracy) and 18 U.S.C. § 2113(b) (bank theft) are currently located on the subject device and in the subject bags. This affidavit further

provides facts to establish probable cause to believe that Roberto Olmos has committed the offenses listed above.

4. Since this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included every fact known to me concerning the investigation. Rather, I have set forth only the facts that I believe are necessary to establish probable cause to authorize a search warrant for the subject device and the subject bages. This affidavit is based on my personal knowledge, as well as information provided by records, databases, and other law enforcement officers.

#### **ATM Jackpotting**

5. ATM “jackpotting” is a relatively new scheme where criminals install malicious software and/or hardware at ATMs that forces the machines to dispense large amounts of cash on demand. Jackpotting often targets financial institutions that operate stand-alone ATMs located inside big-box retailers, gas stations, and convenience stores.

6. To carry out a jackpotting attack, criminals first gain physical access to the upper portion, known commonly as the “top hat,” of the cash machine. They then install malware or specialized electronics — often a combination of both — to control the operations of the ATM.

7. A slight variation of the scheme is known as a “black box” attack. During this type of attack, attackers use a Raspberry Pi device to exploit weaknesses in the ATM’s network connectivity and identify the target system responsible for core functionality of the ATM. This may include the transaction processing system, the cash dispenser module, or the user interface. The attackers then deploy custom software or scripts on the target

system to manipulate its behavior, forcing the ATM to dispense cash. Based on my experience and training, I know that the attackers carry out a well-coordinated attack to withdraw as much cash from the ATM as possible without being detected. The attackers usually use a “cash out crew” of between four to ten individuals. Members of the cash out crew rotate in during the attack to make cash withdrawals while others conduct counter surveillance and attempt to occupy the store associates. I know that the attackers usually stay in constant cellular communication during the jackpotting attacks by wearing earbuds. To avoid detection and to minimize raising suspicion, members of the cash out crew usually spend no longer than ten minutes at the ATM making withdrawals. The attackers often erase any evidence of their presence on the compromised system, including log files, network traces, and any other indicators that may raise suspicion.

8. Criminals often target multiple ATMs in the span of a couple days before fleeing the area with little risk of being caught due to the difficulty of identifying and responding to a jackpotting attack in progress. Jackpotting attacks are often first detected when the financial institution or ATM service provider conducts a reconciliation of the targeted ATM. The reconciliation is often conducted days after the jackpotting attack.

#### **Probable Cause**

9. Since September 2021, TransFund has been the victim of coordinated ATM jackpotting attacks in Oklahoma City and other areas throughout the region. TransFund is a subsidiary of Bank of Oklahoma, and it operates a large ATM network throughout the region. At all times material to this investigation, Bank of Oklahoma was a financial institution, the accounts and deposits of which were insured by the Federal Deposit

Insurance Corporation. As of today, over 100 jackpotting attacks have resulted in losses to Bank of Oklahoma exceeding \$6.5 million.

10. On May 16, 2023, a fraud investigator with Bank of Oklahoma contacted the task force and reported that a group of individuals had successfully jackpotted several TransFund ATMs in Des Moines, Iowa. Each attack occurred inside a Quick Trip convenience store. I reviewed video surveillance from these Quick Trip stores and identified several conspirators, one of whom I later identified as Roberto Olmos, participating in the jackpotting attacks. Between May 9, 2023, and May 11, 2023, the conspirators jackpotted at least six TransFund ATMs in Des Moines, Iowa, defrauding Bank of Oklahoma out of approximately \$320,000.

11. I reviewed surveillance footage from these jackpotting attacks. Each attack took between one to five hours and involved similar conduct by the conspirators. For example, on May 9, 2023, several conspirators jackpotted a TransFund ATM inside a Quick Trip located at 1501 E. Grand Avenue in Des Moines, Iowa. The surveillance footage shows Hector Osornio Manzano apply dark tape over the surveillance camera closest to the ATM. A second camera near the ATM shows Hector Osornio Manzano and a co-conspirator approach the ATM, open the top hat, and then install the hardware. After the installation, Hector Osornio Manzano sees the other surveillance camera near the ATM and immediately applies dark tape over it as well. Over the next four hours, several conspirators, including Roberto Olmos, Dannys Rojas Ramirez, and Johnny Cruz Romero are seen on surveillance cameras inside the store. The conspirators would usually enter the store and walk directly back to the restroom. After several minutes, they would emerge

from the restroom and are seen on surveillance cameras walking across the store to the area where the ATM was located. Based on my experience and training, I believe the conspirators were making cash withdrawals at the ATM as part of the cash out crew. At approximately 7:33 p.m., Hector Osornio Manzano is seen on surveillance camera walking toward the area of the ATM. TransFund electronic journal logs reflect the top hat to the ATM was opened and then closed at 7:33 p.m. Hector Osornio Manzano and Roberto Olmos are seen leaving the store at approximately 7:34 p.m. Bank of Oklahoma confirmed that this TransFund ATM was jackpotted during the time the conspirators were inside the store, causing a loss of \$83,200. Footage obtained from all the attacks in Des Moines was consistent with what I observed at this attack. Members of the same conspiracy were seen on surveillance footage at the other attacks in Des Moines during the time of the attacks. Roberto Olmos was captured on surveillance footage at five of the attacks in Des Moines.

12. Late on May 18, 2023, a fraud investigator with Bank of Oklahoma notified me that a TransFund ATM located inside an OnCue convenience store at 1530 S. Mustang Road in Oklahoma City, Oklahoma, had been jackpotted earlier that day. An OnCue representative reviewed surveillance footage and confirmed that around 4:15 p.m. an individual illegally accessed the top hat of the ATM and appeared to install some type of device inside the ATM. Over the course of the next two hours, a group of individuals made repeated cash withdrawals from the ATM before opening the top hat, removing the device, and then leaving the store.

13. On May 19, 2023, a fraud investigator with Bank of Oklahoma and Task Force Officer Sean Querry inspected the TransFund ATM located inside the OnCue at



1530 S. Mustang Road in Oklahoma City. It confirmed that the locking mechanism to the top hat had been physically manipulated. I then reviewed surveillance from the jackpotting attack, which showed Hector Osornio Manzano manipulating the top hat around 4:00 p.m. on May 18, 2023. While he was installing the black box inside the top hat, Johnny Cruz Romero stood next to him and prevented the OnCue employees from seeing what Hector Osornio Manzano was doing.

14. Hector Osornio Manzano closes the top hat and walks away. Several conspirators make multiple cash withdrawals during the jackpotting attack. For example, at approximately 4:09 p.m., Johnny Cruz Romero withdraws \$5,600 from the ATM. Within minutes, Roberto Olmos withdraws \$5,600. At approximately 5:39 p.m., Hector Osornio Manzano and Johnny Cruz Romero approach the ATM. Johnny Cruz Romero positions himself between the ATM and the OnCue employees while Hector Osornio Manzano opens the top hat and removes the black box before closing the top hat and walking out of the store around 5:42 p.m. Bank of Oklahoma verified that this jackpotting attack caused a \$53,400 loss to the bank.

15. On May 19, 2023, Bank of Oklahoma identified another jackpotting attack that occurred on May 18, 2023, at a TransFund ATM located inside an Oklahoma City OnCue convenience store at 820 S. Meridian Avenue. Bank of Oklahoma determined that this jackpotting attack started around 6:20 p.m. and caused a \$56,520 loss to the bank.

16. On May 19, 2023, a fraud investigator with Bank of Oklahoma and Task Force Officer Sean Query inspected the TransFund ATM located inside the OnCue at 820 S. Meridian Avenue in Oklahoma City. Consistent with the previous attack, the locking



mechanism to the top hat had been physically manipulated. I reviewed surveillance from the jackpotting attack, which showed Hector Osornio Manzano manipulating the top hat around 6:23 p.m. on May 18, 2023. While he was installing the black box inside the top hat, Johnny Cruz Romero stood next to him and prevented the OnCue employees from seeing what Hector Osornio Manzano was doing.

17. Hector Osornio Manzano closes the top hat and walks away. Several conspirators make multiple cash withdrawals during the jackpotting attack. For example, between approximately 6:42 p.m. and 6:49 p.m., Johnny Cruz Romero made several withdrawals. Roberto Olmos then approached the ATM and made several withdrawals before walking away at 6:56 p.m. At approximately 8:16 p.m., Hector Osornio Manzano approached the ATM and then was joined at the ATM by Johnny Cruz Romero. Johnny Cruz Romero positions himself between the ATM and the OnCue employees while Hector Osornio Manzano opens the top hat and removes the black box before closing the top hat and walking out of the store around 8:22 p.m.

18. On July 18, 2023, an Oklahoma County judge issued arrest warrants for Hector Osornio Manzano and Roberto Olmos for conspiracy and felony computer crimes. Late that evening, Hector Osornio Manzano and Roberto Olmos were arrested at the Dallas Fort Worth International Airport where they were scheduled to travel to Mexico City, Mexico.<sup>1</sup> At the time of arrest, Hector Osornio Manzano had approximately \$14,000 in

---

<sup>1</sup> On July 27, 2023, Roberto Olmos and three conspirators were charged by criminal complaint in the Western District of Oklahoma. *United States v. Manzano, et al.*, M-23-566-SM. On September 5, 2023, Roberto Olmos and six conspirators were charged by indictment with,

cash in his possession (\$6,000 in his checked bag and \$8,000 on his person) and Roberto Olmos had \$8,683 in cash on his person. The cash seized from Roberto Olmos consisted of 434 \$20 bills and 3 \$1 bills. Additionally, at the time of arrest, Roberto Olmos had the subject device on his person and was in possession of two of the subject bags. Specifically, he had the brown Delsey Paris backpack and the black and brown Samsonite rolling hardside luggage bag within his reach. Roberto Olmos had previously checked in the blue Samsonite soft luggage bag with the airline when he arrived at the airport. Agents instructed the airline to locate that bag and provide it to them, which they did. The subject device and the subject bags were transported by United States Secret Service agents to the Dallas Field Office and placed in secure storage. The Dallas Field Office forwarded the subject device via UPS to the Oklahoma City Field Office. The subject device arrived on October 23, 2023, and was immediately secured in the evidence vault inside the Oklahoma City Field Office. United States Secret Service agents removed the subject bags from the secure storage at the Dallas Field Office on November 29, 2023, and transported them to the Oklahoma City Field Office where they were placed inside the evidence vault on that same date.

20. Based on my investigation into this conspiracy and into previous ATM jackpotting schemes, I know the conspirators use mobile phones to coordinate the attacks and to stay in constant contact during each attack. The conspirators communicate via text message, phone calls, and various applications, including WhatsApp, to further the attacks.

---

among other charges, conspiracy to commit bank theft. *United States v. Manzano, et al.*, CR-23-373-HE.

During each of the instant attacks, the conspirators, including Roberto Olmos, are caught on video surveillance wearing earbuds. I believe the subject device likely contains communications, pictures, and other evidence of the offenses listed above. Additionally, I believe the subject device contains geolocation data that will show the subject device was at or near the locations of the attacks.

21. I have reviewed video surveillance from each of the attacks committed by the conspirators. Roberto Olmos participated in at least 25 of these attacks. In each attack, he is captured on video surveillance wearing distinct clothing items, including athletic sneakers, shirts, and hats. I believe the subject bags contain items of clothing that will be consistent with that which Roberto Olmos was wearing during these attacks. I further believe that the subject bags likely contain other evidence of the offenses listed above, including proceeds of the crimes, electronic devices, magnetic strip cards, and receipts and other items showing Roberto Olmos was present at or near the ATMs when they were attacked.

### **Technical Terms**

22. Based on my training and experience, I use the following technical terms to convey the following meanings:

- a. *Cellular telephone*: A cellular telephone (or mobile telephone, or wireless telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A cellular telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, cellular telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers

in electronic “address books;” sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Cellular telephones may also include global positioning system (“GPS”) technology for determining the location of the device.

- b. *GPS*: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated “GPS”) consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna’s latitude, longitude, and sometimes altitude with a high level of precision.

23. Based on my knowledge, training, and experience, I know that the phone described in Attachment A, has the capabilities that allow it to serve as cellular telephone and/or GPS navigation device. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device.

#### **Electronic Storage and Forensic Analysis**

24. Based on my knowledge, training, and experience, I know that electronic devices such as the subject device can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some

period of time on the device. This information can sometimes be recovered with forensics tools.

25. *Forensic evidence.* As further described in Attachment A, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described in the warrant, but also forensic evidence that establishes how the subject device was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the subject device because:

- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).
- b. Forensic evidence on a device can also indicate who has used or controlled the device. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence.
- c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

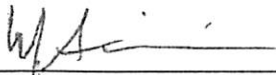
26. *Manner of execution.* Because this warrant only seeks permission to examine the subject devices and the subject bags that are already in law enforcement’s possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

Conclusion

27. Based on the above information, I respectfully submit there is probable cause to believe the subject device and the subject bags described in Attachment A that are located at 210 Park Ave, Suite 1100 in Oklahoma City, Oklahoma, contain evidence of violations of 18 U.S.C. §§ 371 and 2113(b), among others. The items listed in Attachment B are evidence of these crimes, contraband, fruits of these crimes, or property that is or has been used as the means of committing the foregoing offenses.

Therefore, I respectfully request that a search warrant be issued, authorizing the search of the subject device and the subject bags described in Attachment A, and the seizure of the items listed in Attachment B.

FURTHER SAYETH YOUR AFFIANT NOT.

  
\_\_\_\_\_  
Wesley Gillespie  
Special Agent, United States Secret Service

Subscribed and sworn to before me on December 14<sup>th</sup>, 2023.

  
\_\_\_\_\_  
AMANDA MAXFIELD GREEN  
United States Magistrate Judge



**ATTACHMENT A**

**DESCRIPTION OF PROPERTY TO BE SEARCHED**

- 1) A green iPhone 13 Pro Max bearing serial # D479F6MK4C and EMEI # 350776591837361 (“the subject device”)



- 2) A brown Delsey Paris backpack, a black and brown Samsonite rolling hardside luggage bag, and a blue Samsonite soft luggage bag (“the subject bags”)





**ATTACHMENT B**

**DESCRIPTION OF PROPERTY TO BE SEIZED**

Evidence of violations of Title 18, United States Code, Sections 371 and 2113(b), among others, including:

- a. Financial records related to the fraud, however maintained, including bank account records, bank statements, deposit statements/slips, receipts, ledgers, cash receipt books, checks, checkbooks, canceled checks, check registers, withdrawal slips, wire transfers, and cashier's checks.
- b. Receipts, records, and other documents, however maintained, related to past and future travel.
- c. Evidence of travel history, however maintained, including global positioning system location, that provides information on dates, times, and/or location of each subject device.
- d. Directories and/or contacts list, calendars, text messages, multi-media messages, e-mail messages, call logs, photographs, and videos.
- e. Evidence of conspiracy, including communications with phones numbers associated with other individuals or groups involved in criminal activity.
- f. Records of Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.
- g. Evidence of user attribution showing who used or owned the subject devices at the time the items described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history.
- h. Clothing, including hats, which may have been worn while engaged in the crimes.
- i. Proceeds of the crime.
- j. Electronic devices, including Raspberry Pi computers, that could have been used to further the crimes.